PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 :		(11) Numéro de publication internationale:
H04L 9/32	A1	WO 00/64097
		(43) Date de publication internationale: 26 octobre 2000 (26.10.00)

(21) Numéro de la demande internationale: PCT/FR00/01047

(22) Date de dépôt international: 20 avril 2000 (20.04.00)

(30) Données relatives à la priorité:
99/04975 20 avril 1999 (20.04.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: BULL CP8 [FR/FR]; 68, route de Versailles, Boîte postale 45, F–78430 Louveciennes (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: PATARIN, Jacques [FR/FR]; 11, rue Amédée Dailly, F–78220 Viroflay (FR). GOUBIN, Louis [FR/FR]; 3, rue Brown–Séquard, F–75015 Paris (FR).

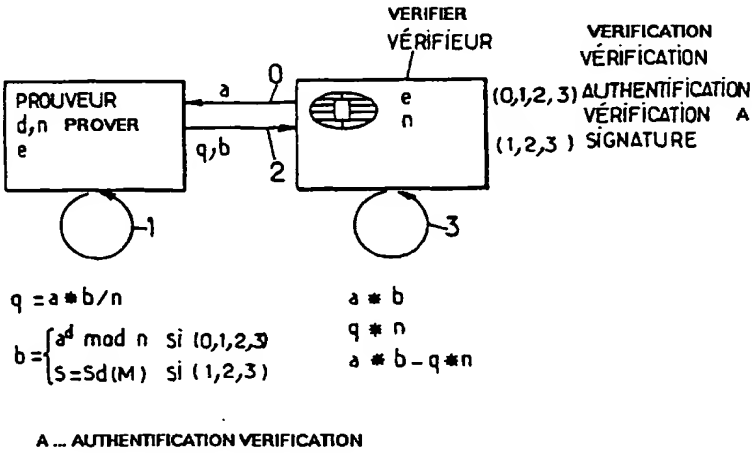
(74) Mandataire: BULL S.A.; Corlu, Bernard, PC58D20, 68, route de Versailles, F–78434 Louveciennes Cedex (FR).

(81) Etats désignés: BR, CN, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: SIGNATURE VERIFICATION AND AUTHENTICATION METHOD

(54) Titre: PROCEDE DE VERIFICATION DE SIGNATURE OU D'AUTHENTIFICATION



A ... AUTHENTIFICATION VERIFICATION

(57) Abstract

The invention concerns a method for verifying signature or authentication between a prover and a verifier based on an asymmetrical cryptographic computational algorithm. The prover computes (1) at least a pre–validation value q, which is a quotient of two cryptographic values a, b, by the public modulo n, and transmits to the verifier said value q. The verifier computes (3) the products a*b and q*n and the difference a*b–q*n to produce at least a modular reduction in the absence of a division operation. The invention is applicable to signature verification and authentication between a proving microcomputer, and a verifying microprocessor card.

(57) Abrégé

L'invention concerne un procédé de vérification de signature ou d'authentification entre prouveur et vérifieur à partir d'un algorithme de calcul cryptographique asymétrique. Le prouveur calcule (1) au moins une valeur de prévalidation q, quotient de deux valeurs cryptographiques a, b par le modulo public n, et transmet au vérifieur cette valeur q. Le vérifieur calcule (3) les produits a*b et q*n et la différence a*b–q*n pour effectuer au moins une réduction modulaire en l'absence d'opération de division. Application à la vérification de signature ou d'authentification entre un prouveur, micro–ordinateur, et un vérifieur, carte à microprocesseur.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

Procédé de vérification de signature ou d'authentification

La présente invention concerne un procédé permettant de rendre plus efficace, en temps de calcul, en RAM et ROM nécessaires, la vérification d'une signature ou d'une authentification asymétrique requérant quelques multiplications modulo n ou des grands nombres.
Les algorithmes de signature ou d'authentification RSA et Rabin sont des exemples permettant la mise en œuvre de ce procédé.

Le procédé est plus particulièrement adapté en vue d'une mise en œuvre dans le cas d'un ordinateur, par exemple un ordinateur personnel désigné par PC, qui génère une signature ou une authentification au moyen d'une clé secrète qui doit ensuite être vérifiée par une carte à microcalculateur. Le microcalculateur effectue cette vérification au moyen d'une clé publique. Il dispose de relativement peu de puissance en comparaison du PC.

Par "*carte à microcalculateur*", on entend un microcontrôleur monolithique standard, avec mémoire incorporée.

Actuellement la majorité des algorithmes à clé publique utilisés dans le monde effectuent des calculs modulo de "*grands nombres*". Par "*grands nombres*", on désigne des nombres entiers positifs et d'au moins 320 bits. Pour des raisons de sécurité, la communauté scientifique recommande même actuellement d'utiliser des nombres d'au moins 512 bits, voire 1024 bits pour la plupart des algorithmes, par exemple pour les algorithmes RSA ou Rabin.

Actuellement les cartes à microcalculateur sont amenées à dialoguer avec des ordinateurs ayant des

capacités de calcul bien plus importantes qu'elles-mêmes. De plus, pour des raisons de coût, on utilise souvent des cartes à microcalculateur sans coprocesseur arithmétique, et avec des ressources en mémoire (ROM, RAM et EEPROM) très limitées. De ce fait, les calculs normalement requis pour réaliser une vérification d'authentification, ou une vérification de signature à clé publique, utilisant des calculs modulo de grands nombres sont souvent très longs, voire impossible faute de mémoire suffisante, si l'on utilise les descriptions traditionnelles des algorithmes cryptographiques.

Dans la suite de la description on désigne par :

- "*prouveur*" : l'entité qui veut être authentifiée, ou qui produit une signature. Elle effectue pour cela des calculs faisant intervenir la clé secrète de l'algorithme asymétrique utilisé. Il s'agira par exemple d'un ordinateur de type PC.
- "*vérifieur*" : l'entité qui vérifie l'authentification, ou qui vérifie la validité d'une signature. Elle effectue pour cela des calculs faisant intervenir uniquement la clé publique de l'algorithme cryptographique asymétrique utilisé. Il s'agira par exemple d'une carte à microcalculateur.

La présente invention a pour objet la mise en œuvre d'un procédé de vérification de signature et d'authentification permettant de remédier aux inconvénients précités inhérents à la capacité de calcul plus limitée d'une entité vérifieur, constituée par une carte à microcalculateur, vis-à-vis d'une entité prouveur, tel qu'un ordinateur personnel ou autre muni d'un dispositif lecteur de carte.

Un autre objet de la présente invention est en conséquence une simplification des opérations de calcul de

certaines réductions modulaires du vérifieur grâce à la mise en œuvre de calculs supplémentaires du prouveur, la tâche du vérifieur étant ainsi simplifiée en l'absence de tout affaiblissement de la sécurité théorique de l'ensemble.

Le procédé de vérification de signature respectivement d'authentification au moyen d'un processus de calcul cryptographique asymétrique à clé privée et à clé publique, objet de la présente invention, ce procédé étant conduit entre une entité *"prouveur"* et une entité *"vérifieur"*, l'entité prouveur effectuant des calculs cryptographiques à partir de la clé privée en vue d'effectuer un calcul de signature, respectivement une valeur d'authentification, et l'entité vérifieur à partir de cette valeur transmise effectuant des calculs cryptographiques à partir de cette clé publique en vue de procéder à cette vérification de signature, respectivement à cette authentification, les opérations de calcul cryptographique mettant en œuvre le calcul de multiplications modulo n ou des grands nombres, est remarquable en ce que, pour un processus de calcul cryptographique mettant en œuvre une clé publique, constituée par un exposant public e et un modulo public n, et une clé privée constituée par un exposant privé, d, ce procédé consiste à calculer, au niveau de l'entité prouveur, au moins une valeur de prévalidation et à transmettre de l'entité prouveur à l'entité vérifieur cette au moins une valeur de prévalidation, permettant à l'entité vérifieur d'effectuer au moins une réduction modulaire en l'absence de toute opération de division pour cette réduction modulaire.

Le procédé, objet de la présente invention, s'applique dans le cadre de tout dialogue ou protocole

d'échange de messages entre une entité prouveur telle qu'un ordinateur personnel et une entité vérifieur telle qu'une carte à microcalculateur, en particulier dans le cadre de transactions bancaires, de contrôle d'accès ou analogue.

Il sera mieux compris à la lecture de la description ci-après et à l'observation des dessins dans lesquels :

- la figure 1 représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre entre une entité prouveur et une entité vérifieur ;

- la figure 2a représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre à partir d'un algorithme de Rabin en vérification d'authentification ;

- la figure 2b représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre à partir d'un algorithme de Rabin en vérification de signature ;

- la figure 3a représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre à partir d'un algorithme RSA en vérification d'authentification ;

- la figure 3b représente un schéma illustratif du procédé, objet de la présente invention, mis en œuvre à partir d'un algorithme RSA en vérification de signature.

Une description plus détaillée du procédé, objet de l'invention, sera donnée en liaison avec la figure 1 et les figures suivantes.

Le procédé objet de l'invention met en œuvre, au niveau de l'entité vérifieur, des algorithmes à clé publique requérant des multiplications modulo n, ou des grands nombres, et les modifie légèrement en faisant faire

le calcul d'un ou de plusieurs quotients q à l'extérieur, c'est-à-dire au niveau de l'entité prouveur, et en fournissant ce ou ces quotients au vérifieur. Ainsi le vérifieur peut plus facilement et plus rapidement calculer certaines multiplications modulaires : au lieu de calculer a*b modulo n, il aura juste à calculer a*b, q*n, et a*b-q*n, a, b désignant des valeurs des calcul de vérification de signature ou d'authentification. Parfois, pour la sécurité il utilise cette dernière valeur d'une façon qui lui permettra de s'assurer que cette dernière valeur est bien comprise entre 1 et n. Lorsque l'on modifie ainsi un algorithme, en "*précalculant*" donc certains quotients, qui sont fournis au vérifieur afin de simplifier les calculs exécutés par ce dernier, on parle d'algorithme "*sous-jacent*" pour désigner l'algorithme initial dont on est parti, avant de faire cette modification. Ainsi, en référence à la figure 1, conformément à un aspect remarquable du procédé objet de la présente invention, le ou les quotients q, vérifiant la relation q=a*b/n, constituent une ou plusieurs valeurs de prévalidation transmises à l'entité vérifieur afin de permettre à l'entité vérifieur d'effectuer au moins une réduction modulaire en l'absence de toute opération de division pour cette réduction modulaire. En référence à la figure 1, on indique que le procédé objet de l'invention peut être mis en œuvre soit en vérification de l'authentification, suite à l'envoi d'une valeur d'incitation tel qu'un aléa a (voir la référence 0 sur la figure), calcul (référence 1) en interne au niveau du prouveur d'une valeur de réponse $b = a^d \bmod n$, et de la valeur de prévalidation q, transmission (référence 2) de b et q du prouveur au vérifieur et calcul (référence 3) par le vérifieur des quantités a*b, q*n et a*b-q*n pour

procéder à la vérification de l'authentification, soit à la vérification de signature d'un message M, suite au calcul (référence 1) au niveau du prouveur d'une signature $S = S_d(M)$ du message M et de la valeur de prévalidation q, envoi (référence 2) du vérifieur au prouveur de q, S et M, calcul (référence 3) au niveau du vérifieur des quantités a*b = S*S, q*n et a*b-q*n pour procéder à la vérification de signature.

Dans la figure 1 et les figures suivantes, une flèche droite représente la transmission des valeurs précitées entre vérifieur et prouveur ou réciproquement et une boucle fléchée au niveau du prouveur ou du vérifieur représente la mise en œuvre d'un calcul interne au niveau du prouveur ou du vérifieur. Enfin, dans la suite de la description, on désigne par réponse R soit la valeur calculée b par chiffrement de l'aléa a dans le cas d'une vérification d'authentification $b = a^d \bmod n$, soit la valeur de signature $S = S_d(M)$ suite à la mise en présence du vérifieur et du prouveur.

Différents exemples de mise en œuvre du procédé objet de la présente invention seront maintenant décrits à partir des algorithmes sous-jacents, désignés par algorithmes RSA et algorithmes de Rabin.

Algorithmes RSA et de Rabin sous-jacents

L'algorithme RSA est le plus célèbre des algorithmes cryptographiques asymétriques. Il a été inventé par RIVEST, SHAMIR et ADLEMAN en 1978. On peut le trouver décrit dans :

R.L. RIVEST, A. SHAMIR, L.M. ADLEMAN : A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 21, n°2, 1978, pp. 120-126.

ou dans les documents suivants :

- ISO/IEC 9594-8/ITU-T X.509, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework ;
- ANSI X9.31-1, American National Standard, Public-Key Cryptography Using Reversible Algorithms for the Financial Services Industry, 1993.

Ces documents sont introduits dans la présente description à titre de référence.

L'algorithme RSA utilise un nombre entier n qui est le produit de deux grands nombres premiers p et r, et un nombre entier e, premier avec ppcm(p-1,r-1), et tel que $e \neq \pm 1$ modulo ppcm(p-1,r-1). Les entiers n et e constituent la clé publique. Le calcul en clé publique fait appel à la fonction α de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ définie par $\alpha(x)=x^e \bmod n$. Le calcul en clé secrète fait appel à la fonction $\alpha^{-1}(y)=y^d \bmod n$, où d est l'exposant secret, appelé aussi *"clé secrète"* ou *"clé privée"*, défini par $ed \equiv 1 \bmod ppcm(p-1,r-1)$.

Notons n le modulo public RSA, notons d l'exposant secret RSA et notons e l'exposant public RSA.

Dans le cas d'une vérification d'authentification, le vérifieur génère un nombre aléatoire A modulo n, et l'envoie au prouveur. Celui ci calcule alors $B= A^d$ modulo n, et renvoie cette valeur B au vérifieur. Celui-ci accepte alors l'authentification si et seulement si:
B^e modulo n = A.

La plus petite valeur de e pour mettre en œuvre l'algorithme RSA est e = 3. Pour e = 2, on parle d'algorithme de Rabin ; celui-ci sera décrit ci-après dans la description. Cette valeur e = 3 est intéressante car elle permet au vérifieur de n'avoir à effectuer que deux multiplications modulaires.

L'algorithme de Rabin est en quelque sorte un algorithme RSA avec l'exposant public e = 2. En fait, lorsque e = 2, la fonction x^e n'est pas bijective modulo n, lorsque n est le produit de deux nombres premiers > 2, on introduit donc des petites modifications dans l'utilisation de l'algorithme de Rabin par rapport au RSA.

On peut trouver une description de l'algorithme de Rabin dans :

M.O. Rabin, Digitized Signatures and Public-Key Functions as intractable as Factorization, Technical Report LCS/TR-212, M.I.T. Laboratory for Computer Science, 1979, introduit dans la présente demande de brevet à titre de référence.

Exemples de mise en œuvre du procédé objet de l'invention à partir des algorithmes de Rabin et RSA

◆ Algorithme de Rabin

Le procédé, objet de la présente invention, sera tout d'abord décrit dans un mode de réalisation particulier non limitatif à partir de l'algorithme de Rabin, soit pour e = 2.

◆◆ Vérification d'authentification

Ainsi que représenté en figure 2a, un exemple possible d'utilisation de l'algorithme de Rabin en vérification d'authentification est maintenant décrit.
Notons n le modulo public. Le vérifieur génère un nombre aléatoire A modulo n, et l'envoie, (référence 0 sur la figure), au prouveur. Celui-ci calcule alors un nombre B (référence 1), et renvoie cette valeur B au vérifieur. Celui-ci accepte alors l'authentification si et seulement si: B*B modulo n est égal à l'une des quatre valeurs possibles suivantes : A, ou n-A, ou C*A modulo n, ou -C*A

modulo n. C est un nombre fixé par le protocole, C = 2 le plus souvent.

Pour simplifier le processus de vérification, conformément au procédé objet de la présente invention, le prouveur n'envoie pas, (référence 2), la valeur B seule : il envoie B et Q, où Q est le quotient de B*B par le modulo public n. Le vérifieur vérifie alors que D_{AR} = B*B - Q*n est bien égal à l'une des quatre valeurs suivantes : A, n-A, (C*A) modulo n, ou (-C*A) modulo n. De plus, il peut calculer (C*A) modulo n en calculant C*A, en gardant cette valeur si elle est < n, et en prenant la valeur C*A - n sinon. De même, il peut calculer (-C*A) modulo n en calculant n-C*A, en gardant cette valeur si elle est >= 0, et en prenant la valeur C*n - C*A sinon. Ainsi le vérifieur n'a plus aucune division à effectuer.

◆◆ Vérification de signature

Ainsi que représenté en figure 2b, et en conservant les mêmes notations que ci-dessus, on note M le message dont le vérifieur souhaite vérifier la signature S. La signature S est obtenue à partir de la clé privée d par S = $S_d(M)$, $S_d(M)$ désignant l'opération de calcul de signature du message M. Si S est une signature Rabin de M, alors le vérifieur vérifie normalement que S*S modulo n = f(M) ou n-f(M), ou (2*f(M) modulo n) ou (-2*f(M) modulo n), où f est une fonction publique standardisée du message M. Par exemple f est la fonction identité, ou bien est décrite dans une norme de signature ; par exemple on peut utiliser les opérations de *paddage* ou concaténation de la norme PKCS#1, établie pour du RSA normalement, confer les éléments descriptifs de cette norme ci-après dans la description.

En conservant les mêmes notations que ci-dessus, pour simplifier le processus de vérification de la

signature, ainsi que représenté en figure 2b, dans le procédé objet de la présente invention, le prouveur n'envoie pas, (référence 2), la valeur S seule : il envoie S et Q, où Q est le quotient de S*S par le modulo public n. Le vérifieur vérifie alors que D_{SR} = S*S - Q*n est bien égal à f(M), ou n-f(M), ou C*f(M) modulo n, ou -C*f(M) modulo n, où C est un nombre fixé par le protocole, C pouvant être pris égal à 2. Comme ces deux dernières valeurs peuvent être calculées modulo n en effectuant zéro ou une soustraction par n, le vérifieur n'a plus aucune division à calculer.

◆ Algorithme RSA

Le procédé, objet de la présente invention, sera maintenant décrit dans un mode de réalisation particulier non limitatif à partir de l'algorithme RSA, soit pour e = 3.

◆◆ Vérification d'authentification

Ainsi que représenté en figure 3a, à partir d'un aléa A, pour simplifier le processus de vérification, dans la présente invention le prouveur n'envoie pas, (référence 2), la valeur B seule : il envoie B, Q1 et Q2, où Q1 est le quotient de B*B par le modulo public n, et où Q2 est le quotient de B*(B*B - Q1*n) par n. Le vérifieur vérifiera alors que D_{ARSA} = B*(B*B - Q1*n) -Q2*n est bien égal à A. Ainsi le vérifieur n'a plus aucune division à effectuer.

◆◆ Vérification de signature

En conservant les mêmes notations que ci-dessus et en notant M le message dont le vérifieur souhaite vérifier la signature S, S est une signature RSA de M, alors le vérifieur vérifie normalement que S^e modulo n = f(M), où f est une fonction publique standardisée du message M. Par exemple f est la fonction identité, ou bien est décrite dans une norme de signature RSA, comme par exemple la

norme PKCS#1. La fonction publique normalisée peut consister à appliquer au message M une fonction de condensation SHA-1 pour obtenir un condensé de message CM, puis à concaténer à ce condensé de message une valeur constante.

Ainsi que représenté en figure 3b, et en conservant les mêmes notations que ci-dessus, pour simplifier le processus de vérification de la signature, dans le procédé, objet de la présente invention, le prouveur n'envoie pas, (référence 2), la valeur S seule : il envoie S, Q1 et Q2, où Q1 est le quotient de S*S par le modulo public n, et où Q2 est le quotient de S*(S*S - Q1*n) par n. Le vérifieur vérifiera alors que D_{SRSA} = S*(S*S - Q1*n) -Q2*n est bien égal à f(M). Ainsi le vérifieur n'a plus aucune division à effectuer.

La fonction de condensation SHA-1 est une fonction publique de "*condensation*". Elle prend en entrée un message dont la taille peut aller de 0 octets à plusieurs Giga octets, et donne en sortie un "*condensé*" du message de 160 bits. Cette fonction est souvent utilisée dans des normes ou avec des algorithmes de signature, car elle est réputée être résistante aux collisions, c'est-à-dire que l'on ne sait pas trouver concrètement deux messages distincts qui ont le même condensé (il en existe mais on ne sait pas comment trouver un tel couple de messages). Ceci permet de signer le condensé des messages plutôt que les messages eux-mêmes.

La norme PKCS#1 est une norme de signature RSA. Elle décrit une fonction publique f. Cette fonction f est appliquée sur le message M à signer avec RSA avant de lancer l'opération d'exponentiation modulaire RSA proprement dite : la signature RSA de M sera donc

S = $(f(M))^d$ modulo n, où n est le modulo public

RSA et où d est l'exposant secret RSA. f utilise une fonction de condensation (par exemple SHA-1) suivie d'un *paddage*, ou concaténation, avec une constante.

Pour une description plus détaillée, on peut consulter :

PKCS#1, RSA *Encryption Standard*, version 2, 1998, disponible à l'adresse suivante :

ftp://ftp.rsa.com/pub/pkcs/doc/pkcs-1v2.doc

dont la version éditée est introduite dans la présente demande à titre de référence.

L'invention consiste ainsi à fournir des données supplémentaires au vérifieur afin de lui faciliter les calculs. Pour précalculer ces données, ici des quotients constituant la ou les valeurs de pré-validation, on n'a pas besoin d'utiliser la clé secrète de l'algorithme. Cela signifie que ces données sont complètement redondantes par rapport aux valeurs transmises à la carte dans une utilisation "*classique*" de l'algorithme asymétrique. En fait, dans la version "classique", la carte sait retrouver elle-même ces quotients. Il n'y a donc aucune information supplémentaire fournie à la carte, au sens de la théorie de l'information, lorsqu'on met en œuvre le procédé, objet de la présente invention tel que décrit précédemment. Cela montre que la sécurité de l'ensemble n'est en rien affaiblie par rapport à la mise en œuvre "*classique*" de l'algorithme.

REVENDICATIONS

1. Procédé de vérification de signature, respectivement d'authentification, au moyen d'un processus de calcul cryptographique asymétrique à clé privée et à clé publique, entre une entité *"prouveur"* et une entité *"vérifieur"*, l'entité prouveur effectuant des calculs cryptographiques à partir de ladite clé privée en vue d'effectuer un calcul de signature, respectivement d'une valeur d'authentification, constituant une valeur de réponse et l'entité vérifieur, à partir de cette valeur de réponse, effectuant des calculs cryptographiques à partir de ladite clé publique en vue de procéder à cette vérification de signature, respectivement cette authentification, les opérations de calcul cryptographique mettant en œuvre le calcul de multiplications modulo n ou des grands nombres, caractérisé en ce que pour un processus de calcul cryptographique mettant en œuvre une clé publique, comprenant un exposant public e et un modulo public n, et une clé privée comprenant un exposant privé, celui-ci comprend les étapes suivantes :

- calculer au niveau de ladite entité prouveur au moins une valeur de pré-validation ;
- transmettre de l'entité prouveur à l'entité vérifieur ladite au moins une valeur de pré-validation, cette valeur de pré-validation permettant à l'entité vérifieur d'effectuer au moins une réduction modulaire en l'absence de toute opération de division pour cette réduction modulaire.

2. Procédé selon la revendication 1, caractérisé en ce que pour un exposant public e=2, le processus de calcul cryptographique étant basé sur un algorithme de RABIN, ladite au moins une valeur de pré-validation comprend une valeur unique, quotient Q du carré de ladite

valeur de signature, respectivement de réponse ,par ledit modulo public n, $Q = R*R/n$, où R désigne ladite valeur de signature, respectivement de réponse, à une authentification.

3. Procédé selon la revendication 2, caractérisé en ce que suite à la réception par ladite entité vérifieur de ladite valeur de réponse à une vérification d'authentification respectivement de signature d'un message (M) et de ladite au moins une valeur de pré-validation, comprenant ledit quotient, ce procédé comprend, au niveau de ladite entité vérifieur, les étapes suivantes :

- calculer la différence (D_{AR}, D_{SR}) entre le carré de la valeur de réponse R*R et le produit Q*n dudit quotient Q par ledit modulo public n,
(D_{AR}, D_{SR}) = R*R -Q*n ;
- vérifier l'égalité de ladite différence avec la valeur d'une fonction de cette valeur de réponse, en l'absence de toute opération de division par l'opération modulo n.

4. Procédé selon la revendication 1, caractérisé en ce que pour un exposant public e = 3, le processus de calcul cryptographique étant basé sur un algorithme RSA, ladite au moins une valeur de pré-validation comprend :

- un premier quotient Q_1 du carré R*R de ladite valeur de réponse R par ledit modulo public n ;
- un deuxième quotient Q_2 du produit de ladite valeur de réponse et de la différence entre le carré R*R de cette valeur de réponse et du produit dudit premier quotient Q_1 et du modulo public n, par ledit modulo public n, $Q_2 = R*(R*R - Q_1*n)/n$.

5. Procédé selon la revendication 4, caractérisé en ce que suite à la réception de ladite valeur de réponse

R et de ladite au moins une valeur de pré-validation comprenant lesdits premier et deuxième quotients Q_1, Q_2, ledit procédé comprend, au niveau de ladite entité vérifieur, les étapes suivantes :

- calculer la différence (D_{ARSA}, D_{SRSA}) entre le produit de ladite valeur de réponse R et de la différence entre le carré R*R de cette valeur de réponse et le produit dudit premier quotient Q_1 et du modulo public n et le produit dudit deuxième quotient Q_2 et dudit modulo public n, (D_{ARSA}, D_{SRSA}) = $R*(R*R - Q_1*n)-Q_2*n$;
- vérifier l'égalité de cette différence avec la valeur d'une fonction de ladite valeur de réponse, en l'absence de toute opération de division par opération modulo n.

6. Procédé selon la revendication 3 ou 5, caractérisé en ce que pour une opération de vérification de signature d'un message (M), ladite fonction comprenant une fonction publique normalisée f(M) de ce message M, il comprend les étapes suivantes :

- appliquer à ce message une fonction de condensation pour obtenir un condensé de message CM ;
- concaténer à ce condensé de message une valeur constante.

7. Procédé selon l'une des revendications 3 ou 5, caractérisé en ce que, pour une opération de vérification d'authentification, ce procédé comprend en outre l'étape de transmission de l'entité vérifieur à l'entité prouveur d'une valeur d'incitation.

8. Procédé selon la revendication 7, caractérisé en ce que ladite valeur d'incitation comprend une valeur aléatoire A modulo n, ladite valeur de réponse R comprend une valeur chiffrée B, et ladite fonction de la valeur de

réponse comprend une fonction f(A) de ladite valeur aléatoire A.

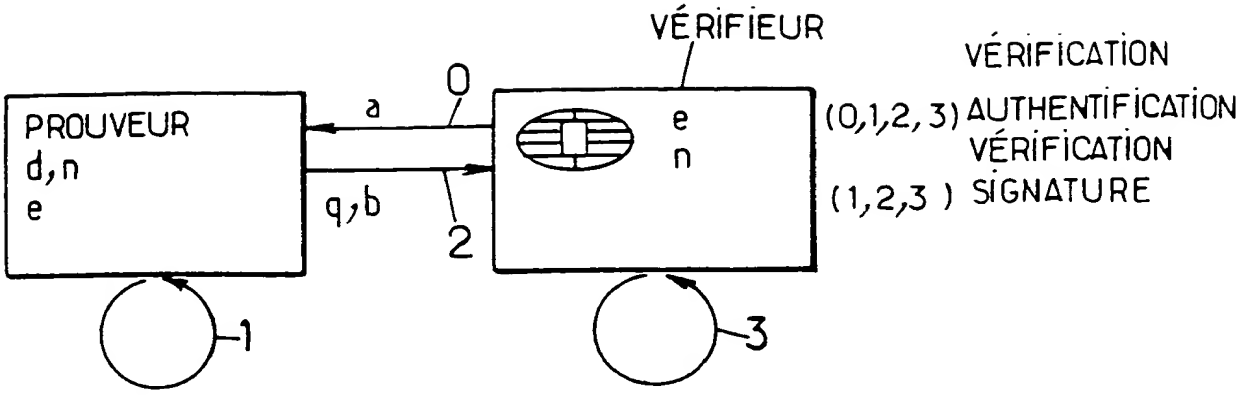
9. Procédé selon l'une des revendications 3 et 7, caractérisé en ce que ladite fonction f(A) de ladite valeur aléatoire A comprend une fonction parmi les fonctions f(A) = A, f(A) = n-A, f(A) = C*A modulo n, f(A) = -C*A modulo n.

10. Procédé selon la revendication 9, caractérisé en ce que, au niveau de l'entité vérifieur, le calcul de ladite fonction f(A) = C*A modulo n comprend le calcul de la valeur C*A et la mémorisation de cette valeur si C*A < n, et le calcul et la mémorisation de la valeur C*A-n sinon, et en ce que le calcul de ladite fonction f(A) = -C*A modulo n comprend le calcul de la valeur n-C*A et la mémorisation de cette valeur si n-C*A ≥ 0, et sinon le calcul de la valeur intermédiaire C*n-C*A, et, si cette valeur intermédiaire est supérieure ou égale à zéro, le calcul et la mémorisation de la valeur de C*n-C*a comme valeur affectée à la valeur de -C*A modulo n, ce qui permet de vérifier l'égalité de ladite authentification en l'absence de toute division pour la réduction modulaire.

11. Procédé selon les revendications 5 et 8, caractérisé en ce que ladite fonction f(A) de ladite valeur aléatoire A est la fonction f(A) = A, ce qui permet de vérifier l'égalité de ladite différence et la validité de ladite authentification, en l'absence d'opération de division pour la réduction modulaire.

12. Procédé selon la revendication 1, caractérisé en ce que ladite valeur de réponse, valeur chiffrée B, et ladite valeur de quotient Q sont concaténées préalablement à leur transmission de l'entité prouveur à l'entité vérifieur.

13. Utilisation du procédé selon la revendication 1, l'entité vérifieur comprenant un système embarqué tel qu'une carte à microprocesseur et l'entité prouveur un système lecteur de système embarqué.



$q = a * b / n$

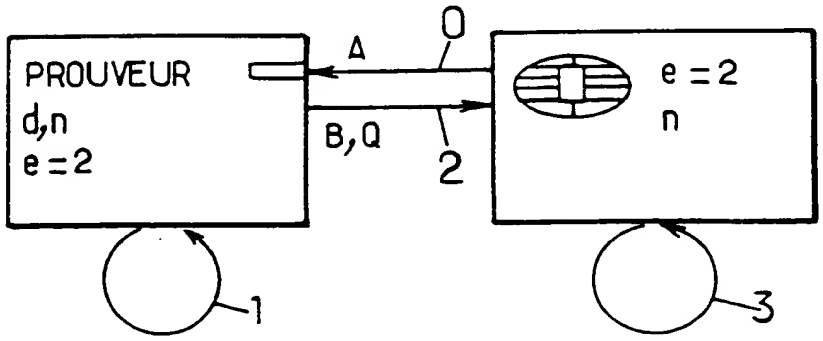
$b = \begin{cases} a^d \bmod n & \text{si } (0,1,2,3) \\ S = Sd(M) & \text{si } (1,2,3) \end{cases}$

$a * b$

$q * n$

$a * b - q * n$

FIG.1.



$R = B = A^d \bmod n$

$Q = B * B / n$

$D_{AR} = B * B - Q * n$

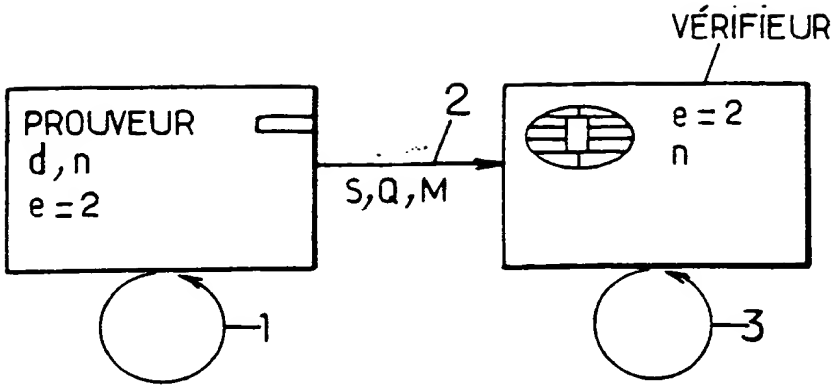
$D_{AR} = A$

$D_{AR} = n - A$

$D_{AR} = C * A \bmod n = C * A$ si $C * A < n$

$D_{AR} = -C * A \bmod n = C * A - n$ SINON

FIG. 2a.



VÉRIFICATION SIGNATURE

$R = S = Sd(M)$

$Q = S * S / n$

$D_{SR} = S * S - Q * n$

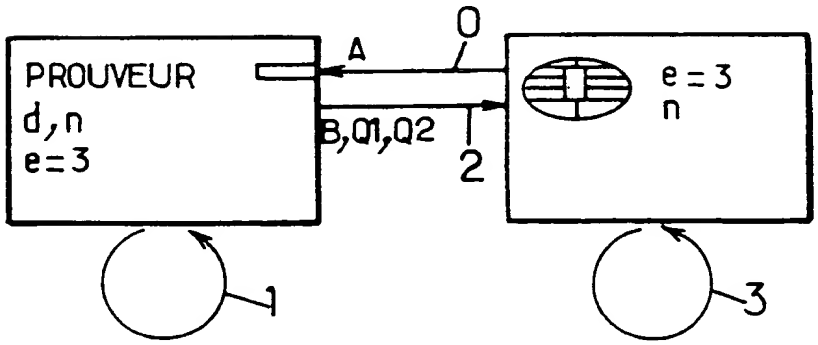
$D_{SR} = f(M)$

$= n - f(M)$

$= C * f(M) \bmod n = C * f(M)$ Si $< n$

$= C * f(M) \bmod n = C * f(M)$ SINON

FIG.2b.



VÉRIFICATION D'AUTHENTIFICATION

$R = B = A^d \bmod n$

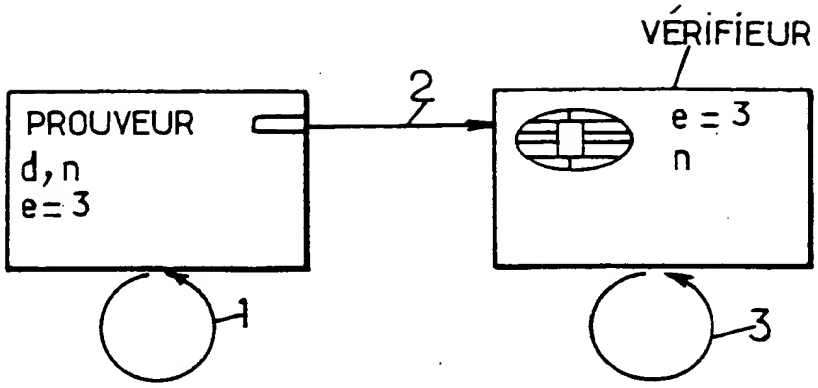
$Q1 = B * B / n$

$Q2 = B(B * B - Q1 * n) / n$

$D_{ARSA} = B(B * B - Q1 * n) - Q2 * n$

$D_{ARSA} = f(A) = A$

FIG.3a.



$R = S = Sd(M)$

$Q1 = S * S / n$

$Q2 = S(S * S - Q1 * n)/n$

$D_{SRSA} = S(S * S - Q1 * n) - Q2 * n$

$D_{SRSA} = f(M)$.

FIG.3b.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 00/01047

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 791 877 A (FRANCE TELECOM) 27 August 1997 (1997-08-27) abstract page 2, line 55 -page 3, line 35 claims 1-6; figure 1	1-5
A	CHANG C C ET AL: "AN ID-BASED SIGNATURE SCHEME BASED UPON RABIN'S PUBLIC KEY CRYPTOSYSTEM" PROCEEDINGS OF THE ANNUAL INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY,US,NEW YORK, IEEE, vol. CONF. 25, 1991, pages 139-141, XP000300422 ISBN: 0-7803-0120-X the whole document	1-5

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 August 2000	09/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 522 473 A (MITSUBISHI ELECTRIC CORP) 13 January 1993 (1993-01-13) abstract page 1, line 2 -page 2, line 19 claims 1,2; figure 1	1

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/01047

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0791877 A	27-08-1997	FR 2745399 A	29-08-1997
EP 0522473 A	13-01-1993	JP 2671649 B	29-10-1997
		JP 5012321 A	22-01-1993
		DE 69224238 D	05-03-1998
		DE 69224238 T	20-05-1998
		US 5245657 A	14-09-1993

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 00/01047

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 791 877 A (FRANCE TELECOM) 27 août 1997 (1997-08-27) abrégé page 2, ligne 55 -page 3, ligne 35 revendications 1-6; figure 1	1-5
A	CHANG C C ET AL: "AN ID-BASED SIGNATURE SCHEME BASED UPON RABIN'S PUBLIC KEY CRYPTOSYSTEM" PROCEEDINGS OF THE ANNUAL INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY,US,NEW YORK, IEEE, vol. CONF. 25, 1991, pages 139-141, XP000300422 ISBN: 0-7803-0120-X le document en entier	1-5

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
2 août 2000	09/08/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Gautier, L

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 522 473 A (MITSUBISHI ELECTRIC CORP) 13 janvier 1993 (1993-01-13) abrégé page 1, ligne 2 -page 2, ligne 19 revendications 1,2; figure 1	1

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 00/01047

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0791877 A	27-08-1997	FR 2745399 A	29-08-1997
EP 0522473 A	13-01-1993	JP 2671649 B	29-10-1997
		JP 5012321 A	22-01-1993
		DE 69224238 D	05-03-1998
		DE 69224238 T	20-05-1998
		US 5245657 A	14-09-1993

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

NOTIFICATION DU NUMÉRO D'ENREGISTREMENT NATIONAL

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Confirmation d'un dépôt par télécopie ☐

À envoyer par l'INPI au demandeur ou au mandataire

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 20 AVR 1999

N° D'ENREGISTREMENT NATIONAL 99 04975

DÉPARTEMENT DE DÉPÔT 75

DATE DE DÉPÔT

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

BULL S.A.
Monsieur Bernard CORLU / PC 58F35
68, route de Versailles
78434 LOUVECIENNES CEDEX

n°du pouvoir permanent	références du correspondant	téléphone
PG 4280	FR3797/BC	01 39.66.61.76

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ▷ demande initiale ◁

☐ certificat d'utilité ☐ transformation d'une demande de brevet européen ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

Procédé de vérification de signature ou d'authentification.

3 DEMANDEUR (S) n° SIREN 3 2 9 5 5 6 1 4 6 code APE-NAF B 3 2 1

Nom et prénoms (souligner le nom patronymique) ou dénomination

BULL CP8

Forme juridique

S.A.

Nationalité (s) **Française**

Adresse (s) complète (s)

BULL CP8
BP 45
68, route de Versailles
78430 LOUVECIENNES

Pays

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

Bernard CORLU
Mandataire -

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

FR 3797/BC

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL

TITRE DE L'INVENTION :

Procédé de vérification de signature ou d'authentification.

LE(S) SOUSSIGNÉ(S)

BULL S.A.

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

Goubin Louis
3 rue Brown Séquard
75015 PARIS
France

Patarin Jacques
11 rue Amédée Dailly
78220 VIROFLAY
France

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Louveciennes, le 16 avril 1999

Corlu Bernard (mandataire)

BA 113/140897

PCT

REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réservé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

Référence du dossier du déposant ou du mandataire *(facultatif)* *(12 caractères au maximum)*: PCT 3797/BC

Cadre n° I TITRE DE L'INVENTION

Procédé de vérification de signature ou d'authentification.

Cadre n° II DÉPOSANT

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

BULL CP8
68, route de Versailles
BP 45
78430 LOUVECIENNES
FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone: (33) 1 39.66.61.76

n° de télécopieur: (33) 1 39.66.61.73

n° de téléimprimeur:

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☒ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

PATARIN Jacques
11 rue Amédée Dailly
78220 VIROFLAY
FRANCE

Cette personne est :
☐ déposant seulement
☒ déposant et inventeur
☐ inventeur seulement
(Si cette case est cochée, ne pas remplir la suite.)

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☒ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

☒ D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme: ☒ mandataire ☐ représentant commun

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)*

BULL S.A
CORLU Bernard
PC58D20 / 68, route de Versailles
F- 78434 LOUVECIENNES Cedex (FRANCE)

n° de téléphone: (33) 1 39.66.61.76

n° de télécopieur: (33) 1 39.66.61.73

n° de téléimprimeur:

☐ **Adresse pour la correspondance :** cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

PCT 754/301299

Feuille n° . . . .

Suite du cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Si aucun des sous-cadres suivants n'est utilisé, cette feuille ne doit pas être incluse dans la requête.

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

GOUBIN Louis
3 rue Brown-Séquard
75015 PARIS
FRANCE

Cette personne est :
☐ déposant seulement
☒ déposant et inventeur
☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) : FRANCE
Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☒ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

Cette personne est :
☐ déposant seulement
☐ déposant et inventeur
☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) :
Domicile (nom de l'État) :

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

Cette personne est :
☐ déposant seulement
☐ déposant et inventeur
☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) :
Domicile (nom de l'État) :

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

Cette personne est :
☐ déposant seulement
☐ déposant et inventeur
☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) :
Domicile (nom de l'État) :

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

☐ D'autres déposants ou inventeurs sont indiqués sur une autre feuille annexe.

Cadre n° V DÉSIGNATION D'ÉTATS

Les désignations suivantes sont faites conformément à la règle 4.9.a) *(cocher les cases appropriées: une au moins doit l'être)* :

Brevet régional

☐ **AP** Brevet ARIPO : GH Ghana, GM Gambie, KE Kenya, LS Lesotho, MW Malawi, SD Soudan, SL Sierra Leone, SZ Swaziland, TZ République-Unie de Tanzanie, UG Ouganda, ZW Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT

☐ **EA** Brevet eurasien : AM Arménie, AZ Azerbaïdjan, BY Bélarus, KG Kirghizistan, KZ Kazakhstan, MD République de Moldova, RU Fédération de Russie, TJ Tadjikistan, TM Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT

☒ **EP** Brevet européen : AT Autriche, BE Belgique, CH et LI Suisse et Liechtenstein, CY Chypre, DE Allemagne, DK Danemark, ES Espagne, FI Finlande, FR France, GB Royaume-Uni, GR Grèce, IE Irlande, IT Italie, LU Luxembourg, MC Monaco, NL Pays-Bas, PT Portugal, SE Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT

☐ **OA** Brevet OAPI : BF Burkina Faso, BJ Bénin, CF République centrafricaine, CG Congo, CI Côte d'Ivoire, CM Cameroun, GA Gabon, GN Guinée, GW Guinée-Bissau, ML Mali, MR Mauritanie, NE Niger, SN Sénégal, TD Tchad, TG Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT *(si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)* . . . . . .

Brevet national *(si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)* :

☐ **AE** Émirats arabes unis
☐ **AL** Albanie . . . . . .
☐ **AM** Arménie . . . . . .
☐ **AT** Autriche . . . . . .
☐ **AU** Australie . . . . . .
☐ **AZ** Azerbaïdjan
☐ **BA** Bosnie-Herzégovine . . . . . .
☐ **BB** Barbade
☐ **BG** Bulgarie . . . . . .
☒ **BR** Brésil . . . . . .
☐ **BY** Bélarus . . . . . .
☐ **CA** Canada
☐ **CH et LI** Suisse et Liechtenstein
☒ **CN** Chine . . . . . .
☐ **CR** Costa Rica . . . . . .
☐ **CU** Cuba . . . . . .
☐ **CZ** République tchèque . . . . . .
☐ **DE** Allemagne . . . . . .
☐ **DK** Danemark . . . . . .
☐ **DM** Dominique
☐ **EE** Estonie . . . . . .
☐ **ES** Espagne . . . . . .
☐ **FI** Finlande . . . . . .
☐ **GB** Royaume-Uni
☐ **GD** Grenade
☐ **GE** Géorgie . . . . . .
☐ **GH** Ghana . . . . . .
☐ **GM** Gambie
☐ **HR** Croatie . . . . . .
☐ **HU** Hongrie . . . . . .
☐ **ID** Indonésie
☐ **IL** Israël . . . . . .
☐ **IN** Inde . . . . . .
☐ **IS** Islande
☒ **JP** Japon . . . . . .
☐ **KE** Kenya . . . . . .
☐ **KG** Kirghizistan . . . . . .
☐ **KP** République populaire démocratique de Corée . . . . . .
☐ **KR** République de Corée . . . . . .
☐ **KZ** Kazakhstan . . . . . .
☐ **LC** Sainte-Lucie
☐ **LK** Sri Lanka
☐ **LR** Liberia
☐ **LS** Lesotho . . . . . .
☐ **LT** Lituanie
☐ **LU** Luxembourg
☐ **LV** Lettonie
☐ **MA** Maroc . . . . . .
☐ **MD** République de Moldova . . . . . .
☐ **MG** Madagascar . . . . . .
☐ **MK** Ex-République yougoslave de Macédoine . . . . . .
☐ **MN** Mongolie
☐ **MW** Malawi . . . . . .
☐ **MX** Mexique . . . . . .
☐ **NO** Norvège
☐ **NZ** Nouvelle-Zélande . . . . . .
☐ **PL** Pologne . . . . . .
☐ **PT** Portugal . . . . . .
☐ **RO** Roumanie
☐ **RU** Fédération de Russie . . . . . .
☐ **SD** Soudan
☐ **SE** Suède
☐ **SG** Singapour
☐ **SI** Slovénie . . . . . .
☐ **SK** Slovaquie . . . . . .
☐ **SL** Sierra Leone . . . . . .
☐ **TJ** Tadjikistan . . . . . .
☐ **TM** Turkménistan . . . . . .
☐ **TR** Turquie . . . . . .
☐ **TT** Trinité-et-Tobago . . . . . .
☐ **TZ** République-Unie de Tanzanie
☐ **UA** Ukraine . . . . . .
☐ **UG** Ouganda . . . . . .
☒ **US** États-Unis d'Amérique . . . . . .
☐ **UZ** Ouzbékistan . . . . . .
☐ **VN** Viet Nam . . . . . .
☐ **YU** Yougoslavie . . . . . .
☐ **ZA** Afrique du Sud . . . . . .
☐ **ZW** Zimbabwe . . . . . .

Cases réservées pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille :

☐ . . . . . .
☐ . . . . . .

Déclaration concernant les désignations de précaution : outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. *(La confirmation (y compris les taxes) doit parvenir à l'office récepteur dans le délai de 15 mois.)*

Cadre n° VI REVENDICATION DE PRIORITÉ ☐ D'autres revendications de priorité sont indiquées dans le cadre supplémentaire.

Date de dépôt de la demande antérieure *(jour/mois/année)*	Numéro de la demande antérieure	Lorsque la demande antérieure est une : demande nationale : pays	demande régionale :* office régional	demande internationale : office récepteur
(1) 20 avril 1999 (20.04.1999)	99 04975	FRANCE		
(2)				
(3)				

☒ L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures *(seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur)* indiquées ci-dessus au(x) point(s) : 1

** Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b)ii)). Voir le cadre supplémentaire.*

Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Choix de l'administration chargée de la recherche internationale (ISA) *(si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé)* : ISA/

Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche *(si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière)* :

Date *(jour/mois/année)*	Numéro	Pays *(ou office régional)*
20.04.99	99 04975 FA 578138	FR

Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT

La présente demande internationale contient le **nombre de feuilles** suivant :

requête	04
description (sauf partie réservée au listage des séquences)	12
revendications	05
abrégé	01
dessins	03
partie de la description réservée au listage des séquences	
Nombre total de feuilles	25

Le ou les éléments cochés ci-après **sont joints** à la présente demande internationale :

1. ☐ feuille de calcul des taxes
2. ☒ pouvoir distinct signé
3. ☐ copie du pouvoir général; numéro de référence, le cas échéant :
4. ☐ explication de l'absence d'une signature
5. ☒ document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) : 1
6. ☐ traduction de la demande internationale en (langue) :
7. ☐ indications séparées concernant des micro-organismes ou autre matériel biologique déposés
8. ☐ listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur
9. ☒ autres éléments *(préciser)* : Rapport de Recherche FA 578138

Figure des dessins qui doit accompagner l'abrégé : 1

Langue de dépôt de la demande internationale : FRANCAIS

Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE

À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.

CORLU Bernard (mandataire)

Réservé à l'office récepteur

1. Date effective de réception des pièces supposées constituer la demande internationale :
2. Dessins : ☐ reçus : ☐ non reçus :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA/
6. ☐ Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international

Date de réception de l'exemplaire original par le Bureau international :

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE LA RECEPTION DE L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT)

Destinataire:

Direction de la Propriété Intellectuelle
- 5 JUIL. 2000
BULL S.A.

BULL S.A.
Corlu, Bernard
PC58D20
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année)	NOTIFICATION IMPORTANTE
15 juin 2000 (15.06.00)	
Référence du dossier du déposant ou du mandataire	**Demande internationale no**
PCT 3797/BC	PCT/FR00/01047

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

BULL CP8 (pour tous les Etats désignés sauf US)
PATARIN, Jacques etc. (pour US seulement)

Date du dépôt international	:	20 avril 2000 (20.04.00)
Date(s) de priorité revendiquée(s)	:	20 avril 1999 (20.04.99)
Date de réception de l'exemplaire original par le Bureau international	:	22 mai 2000 (22.05.00)
Liste des offices désignés	:	

EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
National :BR,CN,JP,US

ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- [X] les délais dans lesquels doit être abordée la phase nationale
- [X] la confirmation des désignations faites par mesure de précaution
- [ ] les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

n° de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé
Dorothée Mülhausen

n° de téléphone (41-22) 338.83.38

Ivu BC

RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE LA PHASE NATIONALE

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de **20 MOIS** à compter dela date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire international ou dans une élection ultérieure, de **30 MOIS** à compter de la date de priorité, à condition que cette électionait été effectuée avant l'expiration du 19e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. **Il appartient au déposant** de veiller à remplir en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 6 septembre1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 6 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

Veuillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation , il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.

EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur : le BUREAU INTERNATIONAL

PCT

NOTIFICATION RELATIVE A LA PRESENTATION OU A LA TRANSMISSION DU DOCUMENT DE PRIORITE

(instruction administrative 411 du PCT)

Destinataire:

BULL S.A.
Corlu, Bernard
PC58D20
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année) 15 juin 2000 (15.06.00)	
Référence du dossier du déposant ou du mandataire PCT 3797/BC	**NOTIFICATION IMPORTANTE**
Demande internationale no PCT/FR00/01047	Date du dépôt international (jour/mois/année) 20 avril 2000 (20.04.00)
Date de publication internationale (jour/mois/année) Pas encore publiée	Date de priorité (jour/mois/année) 20 avril 1999 (20.04.99)
Déposant BULL CP8 etc	

1. La date de réception (sauf lorsque les lettres "NR" figurent dans la colonne de droite) par le Bureau international du ou des documents de priorité correspondant à la ou aux demandes énumérées ci-après est notifiée au déposant. Sauf indication contraire consistant en un astérisque figurant à côté d'une date de réception, ou les lettres "NR", dans la colonne de droite, le document de priorité en question a été présenté ou transmis au Bureau international d'une manière conforme à la règle 17.1.a) ou b).
2. Ce formulaire met à jour et remplace toute notification relative à la présentation ou à la transmission du document de priorité qui a été envoyée précédemment.
3. Un **astérisque(*)** figurant à côté d'une date de réception dans la colonne de droite signale un document de priorité présenté ou transmis au Bureau international mais de manière non conforme à la règle 17.1.a) ou b). Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.
4. Les **lettres "NR"** figurant dans la colonne de droite signalent un document de priorité que le Bureau international n'a pas reçu ou que le déposant n'a pas demandé à l'office récepteur de préparer et de transmettre au Bureau international, conformément à la règle 17.1.a) ou b), respectivement. Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Date de priorité	Demande de priorité n°	Pays, office régional ou office récepteur selon le PCT	Date de réception du document de priorité
20 avri 1999 (20.04.99)	99/04975	FR	22 mai 2000 (22.05.00)

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:
Dorothée Mülhausen

no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT)

Destinataire:
BULL S.A.
Corlu, Bernard
PC58D20
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Direction de la Propriété Intellectuelle
03 NOV. 2000
BULL S.A.

Date d'expédition (jour/mois/année) 26 octobre 2000 (26.10.00)	
Référence du dossier du déposant ou du mandataire PCT 3797/BC	**AVIS IMPORTANT**

Demande internationale no	**Date du dépôt international** (jour/mois/année)	**Date de priorité** (jour/mois/année)
PCT/FR00/01047	20 avril 2000 (20.04.00)	20 avril 1999 (20.04.99)

Déposant
BULL CP8 etc

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:
   US

   Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:
   BR,CN,EP,JP

   La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le
   26 octobre 2000 (26.10.00) sous le numéro WO 00/64097

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, **la demande d'examen préliminaire international** doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé
J. Zahra

no de téléphone (41-22) 338.83.38

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/32	A1	(11) Numéro de publication internationale: **WO 00/64097**
		(43) Date de publication internationale: 26 octobre 2000 (26.10.00)

(21) Numéro de la demande internationale: PCT/FR00/01047

(22) Date de dépôt international: 20 avril 2000 (20.04.00)

(30) Données relatives à la priorité:
99/04975 20 avril 1999 (20.04.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: BULL CP8 [FR/FR]; 68, route de Versailles, Boîte postale 45, F–78430 Louveciennes (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: PATARIN, Jacques [FR/FR]; 11, rue Amédée Dailly, F–78220 Viroflay (FR). GOUBIN, Louis [FR/FR]; 3, rue Brown–Séquard, F–75015 Paris (FR).

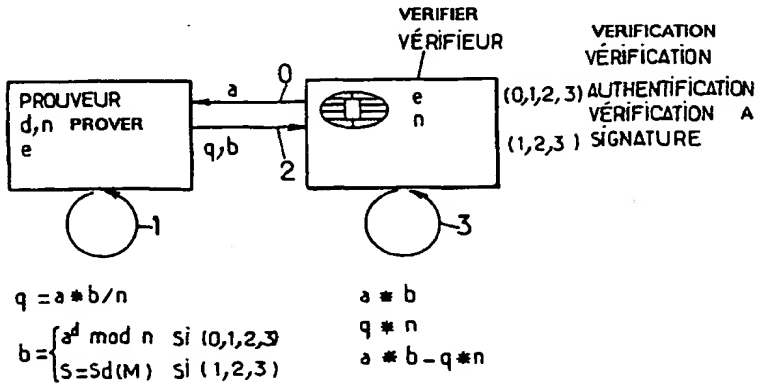
(74) Mandataire: BULL S.A.; Corlu, Bernard, PC58D20, 68, route de Versailles, F–78434 Louveciennes Cedex (FR).

(81) Etats désignés: BR, CN, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: SIGNATURE VERIFICATION AND AUTHENTICATION METHOD

(54) Titre: PROCEDE DE VERIFICATION DE SIGNATURE OU D'AUTHENTIFICATION



A ... AUTHENTIFICATION VERIFICATION

(57) Abstract

The invention concerns a method for verifying signature or authentication between a prover and a verifier based on an asymmetrical cryptographic computational algorithm. The prover computes (1) at least a pre–validation value q, which is a quotient of two cryptographic values a, b, by the public modulo n, and transmits to the verifier said value q. The verifier computes (3) the products a*b and q*n and the difference a*b–q*n to produce at least a modular reduction in the absence of a division operation. The invention is applicable to signature verification and authentication between a proving microcomputer, and a verifying microprocessor card.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
PCT 3797/BC		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 01047	20/04/2000	20/04/1999
Déposant		
BULL CP8		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 1

   [X] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 00/01047

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 791 877 A (FRANCE TELECOM) 27 août 1997 (1997-08-27) abrégé page 2, ligne 55 -page 3, ligne 35 revendications 1-6; figure 1	1-5
A	CHANG C C ET AL: "AN ID-BASED SIGNATURE SCHEME BASED UPON RABIN'S PUBLIC KEY CRYPTOSYSTEM" PROCEEDINGS OF THE ANNUAL INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY,US,NEW YORK, IEEE, vol. CONF. 25, 1991, pages 139-141, XP000300422 ISBN: 0-7803-0120-X le document en entier	1-5

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
2 août 2000	09/08/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 522 473 A (MITSUBISHI ELECTRIC CORP) 13 janvier 1993 (1993-01-13) abrégé page 1, ligne 2 -page 2, ligne 19 revendications 1,2; figure 1	1

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/01047

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0791877 A	27-08-1997	FR 2745399 A	29-08-1997
EP 0522473 A	13-01-1993	JP 2671649 B	29-10-1997
		JP 5012321 A	22-01-1993
		DE 69224238 D	05-03-1998
		DE 69224238 T	20-05-1998
		US 5245657 A	14-09-1993

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No
PCT/FR 00/01047

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 791 877 A (FRANCE TELECOM) 27 août 1997 (1997-08-27) abrégé page 2, ligne 55 -page 3, ligne 35 revendications 1-6; figure 1	1-5
A	CHANG C C ET AL: "AN ID-BASED SIGNATURE SCHEME BASED UPON RABIN'S PUBLIC KEY CRYPTOSYSTEM" PROCEEDINGS OF THE ANNUAL INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY,US,NEW YORK, IEEE, vol. CONF. 25, 1991, pages 139-141, XP000300422 ISBN: 0-7803-0120-X le document en entier	1-5

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
2 août 2000	09/08/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Gautier, L

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 522 473 A (MITSUBISHI ELECTRIC CORP) 13 janvier 1993 (1993-01-13) abrégé page 1, ligne 2 -page 2, ligne 19 revendications 1,2; figure 1	1

1

RAPPORT DE RECHERCHE [redacted]ERNATIONALE

Renseignements relatifs a[redacted] membres de familles de brevets

Demande Internationale No
PCT/FR 00/01047

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0791877 A	27-08-1997	FR 2745399 A	29-08-1997
EP 0522473 A	13-01-1993	JP 2671649 B	29-10-1997
		JP 5012321 A	22-01-1993
		DE 69224238 D	05-03-1998
		DE 69224238 T	20-05-1998
		US 5245657 A	14-09-1993